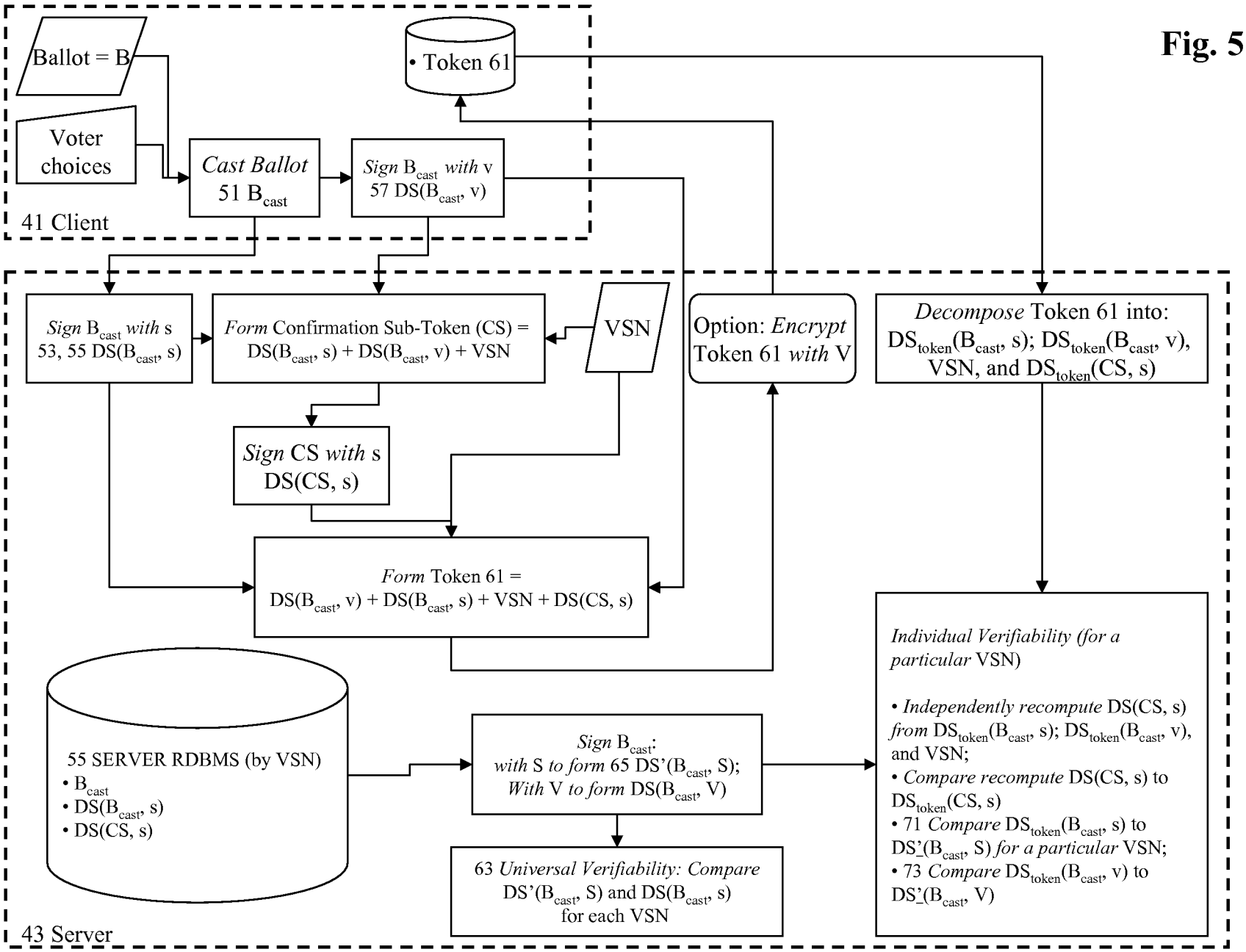
Fig. 5


Ballot = B
• Token 61
Voter choices
Cast Ballot 51 B_{cast}
Sign B_{cast} with v 57 $DS(B_{cast}, v)$
41 Client
Sign B_{cast} with s 53, 55 $DS(B_{cast}, s)$
Form Confirmation Sub-Token (CS) = $DS(B_{cast}, s) + DS(B_{cast}, v) + VSN$
VSN
Option: Encrypt Token 61 with V
Decompose Token 61 into: $DS_{token}(B_{cast}, s)$; $DS_{token}(B_{cast}, v)$, VSN, and $DS_{token}(CS, s)$
Sign CS with s DS(CS, s)
Form Token 61 = $DS(B_{cast}, v) + DS(B_{cast}, s) + VSN + DS(CS, s)$
55 SERVER RDBMS (by VSN)
• B_{cast}
• $DS(B_{cast}, s)$
• DS(CS, s)
Sign B_{cast}: with S to form 65 $DS'(B_{cast}, S)$; With V to form $DS(B_{cast}, V)$
63 Universal Verifiability: Compare $DS'(B_{cast}, S)$ and $DS(B_{cast}, s)$ for each VSN
Individual Verifiability (for a particular VSN)
• Independently recompute DS(CS, s) from $DS_{token}(B_{cast}, s)$; $DS_{token}(B_{cast}, v)$, and VSN;
• Compare recompute DS(CS, s) to $DS_{token}(CS, s)$
• 71 Compare $DS_{token}(B_{cast}, s)$ to $DS'(B_{cast}, S)$ for a particular VSN;
• 73 Compare $DS_{token}(B_{cast}, v)$ to $DS'(B_{cast}, V)$
43 Server